A Group of Integral Points in a Matrix Parallelepiped

Ken Byrd and Theresa P. Vaughan
Department of Mathematics
University of North Carolina at Greensboro
Greensboro, North Carolina 27412

Submitted by Hans Scheider

ABSTRACT

Let A be an $n\times n$ integral matrix with determinant $D>0$, and let $P(A)$ be the n-parallelepiped determined by the columns $\{A_i\}_{i=1}^n$ of A,

$$P(A)=\left\{\sum_{i=1}^{n} x_iA_i \,\middle|\, 0\leqslant x_i\leqslant 1\right\}.$$

Let L be the set of integral vectors in $P(A)$, and let $G(A)$ be the subset of L consisting of vectors whose coefficients x_i satisfy $0\leqslant x_i<1$. We show that $G(A)$, equipped with addition modulo 1 on the coefficients x_i, is an Abelian group of order D, whose invariant factors are the invariant factors of the integral matrix A. We give a formula for $|L|$, and show that $|L|$ is not a similarity invariant.

1. INTRODUCTION

Let A be an $n\times n$ integral matrix with determinant $D>0$, and let $P(A)$ be the n-parallelepiped in Euclidean n-space determined by the columns $\{A_i\}_{i=1}^n$ of A:

$$P(A)=\left\{\sum_{i=1}^{n} x_iA_i \,\middle|\, 0\leqslant x_i\leqslant 1\right\}.$$

In this paper we are concerned with the integral points in $P(A)$, that is, with vectors $v=(v_1,v_2,\ldots,v_n)\in P(A)$ where the entries v_i are integers. Let

$$L=\left\{v=\sum_{i=1}^{n} x_iA_i \,\middle|\, 0\leqslant x_i\leqslant 1;\ v \text{ integral}\right\},$$

$$G(A)=\left\{v=\sum_{i=1}^{n} x_iA_i \,\middle|\, 0\leqslant x_i<1;\ v \text{ integral}\right\}.$$

 0024-3795/80/020155+12$01.75

In Sec. 2 we show that $G(A)$, equipped with a natural addition, is an Abelian group. In Sec. 3 we show that the order of $G(A)$ is D, and that the invariant factors of $G(A)$ (as an Abelian group) are precisely the invariant factors of A (as an integral matrix).

The nonzero vertices of $P(A)$ are not in $G(A)$, so that $G(A) \neq L$. In Sec. 4 we show how to find the cardinality of L, and in Sec. 5 an example is given to show that $|L|$ is not a similarity invariant. Finally, in Sec. 5 we give an example to illustrate the results of this paper.

2. DEFINITIONS AND PRELIMINARIES

Throughout this section we assume that A is an $n \times n$ integral matrix with determinant $D > 0$, whose columns are $\{A_i\}_{i=1}^n$. Let $P(A)$ be the n-parallelepiped in $\mathbb{R}^n$ determined by the columns of A:

$$P(A) = \left\{ \sum_{i=1}^{n} x_i A_i \,\middle|\, 0 \leqslant x_i \leqslant 1 \right\}.$$

DEFINITION 2.1. Let

$$X = \sum_{i=1}^{n} x_i A_i \qquad (0 \leqslant x_i \leqslant 1).$$

The x_i are called the coefficients of X. If $0 \leqslant x_i < 1$ for $i = 1, 2, \ldots, n$, we say that X is in *reduced form*. Let $G(A)$ be the set of all integral vectors in $P(A)$ which are in reduced form:

$$G(A) = \left\{ v = \sum_{i=1}^{n} x_i A_i \,\middle|\, 0 \leqslant x_i < 1;\ v \text{ integral} \right\}.$$

Define an operation $\oplus$ on $G(A)$ by

$$\sum_{i=1}^{n} x_i A_i \oplus \sum_{i=1}^{n} y_i A_i = \sum_{i=1}^{n} z_i A_i,$$

where

$$z_i = \begin{cases} x_i + y_i & \text{if } 0 \leqslant x_i + y_i < 1, \\ x_i + y_i - 1 & \text{if } 1 \leqslant x_i + y_i < 2. \end{cases}$$

Thus, $\oplus$ amounts to addition modulo 1, on the coefficients of the vectors in $G(A)$.

THEOREM 2.2. *The set $G(A)$, equipped with the operation $\oplus$, is a finite Abelian group.*

Proof. Since $\{A_i\}$ is a basis for $\mathbb{R}^n$, the representations $\sum_{i=1}^n x_i A_i$ are unique, so the operation $\oplus$ is well defined. The identity 0 is in $G(A)$, and the additive inverse of

$$X = \sum_{i=1}^{n} x_i A_i \qquad (0 \leqslant x_i < 1)$$

is

$$Y = \sum_{i=1}^{n} y_i A_i,$$

where

$$y_i = \begin{cases} 1 - x_i & \text{if } 0 < x_i < 1, \\ 0 & \text{if } x_i = 0 \end{cases}$$

(clearly if X is integral, so is Y). The associative and commutative laws are obvious. $G(A)$ is finite, since it is a set of integral points in the bounded set $P(A)$. ∎

DEFINITION 2.3. The group $G(A)$ is written additively, and we use the notation $n \odot X$ to represent the sum $X \oplus X \oplus \cdots \oplus X$ (with n summands), for $X \in G(A)$. If we think of X as a vector in $\mathbb{R}^n$, then nX denotes the usual scalar multiplication.

For convenience, we state the next result.

LEMMA 2.4. *Let $X = \sum_{i=1}^n x_i A_i \in G(A)$, and let $k > 0$ be an integer. Then $k \odot X = 0$ (in $G(A)$) if and only if $k(x_1, x_2, \ldots, x_n)$ is an integral vector in $\mathbb{R}^n$, i.e., kX has all integral coefficients.*

The next theorems give a partial description of the elements of $G(A)$.

THEOREM 2.5. *Let* $X \in G(A)$. *Then*

$$X = \sum_{i=1}^{n} \frac{a_i}{b_i} A_i \qquad \left(0 \leqslant \frac{a_i}{b_i} < 1\right),$$

where for $i = 1,2,\ldots,n$, a_i *and* b_i *are integers,* $(a_i, b_i) = 1$, $b_i > 0$, $a_i \geqslant 0$. *If* k *is the order of* X *in* $G(A)$, *then* $k = \operatorname{lcm}\{b_i\}$.

Proof. Since $G(A)$ is finite, then X has some finite order, say k. Then $k \odot X = 0$, or kX has all integral coefficients. But

$$kX = \sum_{i=1}^{n} (kx_i)A_i$$

and (for $i = 1,2,\ldots,n$) kx_i is integral if and only if x_i is rational, $x_i = a_i/b_i, b_i \neq 0$, and $b_i \mid k$. We assume $(a_i, b_i) = 1$. Clearly $\operatorname{lcm}\{b_i\}$ divides k, and now, since $(\operatorname{lcm}\{b_i\})X$ has all integral coefficients, we have $(\operatorname{lcm}\{b_i\}) \odot X = 0$ and $k \mid \operatorname{lcm}\{b_i\}$. So $k = \operatorname{lcm}\{b_i\}$. ∎

THEOREM 2.6. *Let* $X \in G(A)$, *say*

$$X = \sum_{i=1}^{n} \frac{a_i}{b_i} A_i \qquad \left(0 \leqslant \frac{a_i}{b_i} < 1\right).$$

Then for $i = 1,2,\ldots,n$, $b_i \mid D$. *If* k *is the order of* X, *then* $k \mid D$. *On the other hand, if* $p \mid D$, *where* p *is prime, then* $G(A)$ *contains a point* X *of order* p.

Proof. Put $v = (a_1/b_1,\ldots,a_n/b_n)$. Then $X = Av$, so $A^{-1}X = v$. That is

$$\frac{1}{D}(\operatorname{adj} A)X = v.$$

Now $\operatorname{adj} A$ and X are integral, and it is clear that every $b_i \mid D$ $(i = 1,2,\ldots,n)$. Since $k = \operatorname{lcm}\{b_i\}$, then $k \mid D$. To see the last statement, consider the matrix $\bar{A}$, whose entries are the entries of A reduced modulo p. Then $\det \bar{A} = \bar{D} = 0 \pmod{p}$. But now $\bar{A}$ represents a linear transformation of $\mathrm{GF}(p)^n$, and is singular. That is, some combination

$$\sum_{i=1}^{n} r_i \bar{A}_i = 0 \bmod p \qquad (r_i \text{ integers}, \quad 0 \leqslant r_i < p)$$

with not all $r_i \equiv 0 \pmod{p}$. That is,

$$\sum_{i=1}^{n} r_i A_i = p \cdot v$$

for some integral vector v. From the conditions on the r_i, we see that the reduced form of v is a point of order p in $G(A)$. ∎

There is an alternate proof of the last part of this theorem, which is more constructive, since

$$\det(\operatorname{adj} A) = (\det A)^{n-1} = D^{n-1},$$

and if $p^t \mid D$ and $p^{t+1} \nmid D$, there is some column, say $T_i = (t_1, t_2, \ldots, t_n)$, of $\operatorname{adj} A$ such that

$$p^t \nmid \gcd\{t_i\}_{i=1}^{n}.$$

(Otherwise $p^{nt} \mid D^{n-1}$, a contradiction.) If e_i is the ith member of the standard basis, we have

$$\frac{1}{D} A T_i = e_i$$

and if we write $t_i/D = a_i/b_i$, in lowest terms, the condition $p^t \nmid \gcd\{t_i\}$ implies at least one of the b_i is p^k for some $k \geqslant 1$. Then

$$X = \sum_{i=1}^{n} \frac{a_i}{b_i} A_i = e_i$$

has order divisible by p^k, and from this we get a point of order p in $G(A)$.

COROLLARY 2.7. *$D = \pm 1$ if and only if $G(A) = \{0\}$, hence if and only if the only integral points in $P(A)$ are its vertices.*

COROLLARY 2.8. *$D = \pm 1$ if and only if whenever $Av = w$ is an integral vector, then v is also integral; that is, if and only if $A^{-1}(\mathbf{Z}^n) = \mathbf{Z}^n$.*

REMARK 2.9. All of our results apply equally well to integral matrices with negative determinant, for a change of sign of the determinant may be effected by an interchange of columns.

3. THE STRUCTURE OF THE GROUP $G(A)$

As before, A is a fixed $n \times n$ integral matrix with columns $\{A_i\}_{i=1}^n$ and determinant $D > 0$. Let S denote the Smith normal form of A over $\mathbf{Z}$, so that we have

$$PAQ = S = \operatorname{diag}(d_1, d_2, \ldots, d_n),$$

where P and Q are unimodular integral matrices, $d_i \mid d_{i+1}$ $(i = 1, 2, \ldots, n-1)$, and $d_1 d_2 \cdots d_n = D$. The integers $d_1, d_2, \ldots, d_n$ are called the invariant factors of A.

Let $\{Q_i\}_{i=1}^n$ denote the columns of Q. Put $T = P^{-1}$, and let T_i' be the reduced form of column T_i of T.

THEOREM 3.1.

(a) *The set* $\{T_i' \mid d_i > 1\}$ *is a basis for* $G(A)$ *as an Abelian group.*
(b) $G(A) \cong \mathbf{Z}_{d_1} \oplus \mathbf{Z}_{d_2} \oplus \cdots \oplus \mathbf{Z}_{d_n}$
(c) *The order of* $G(A)$ *is* D.

Proof. (a): Since $AQ = TS$, then (column by column)

$$AQ_j = d_j T_j \qquad (j = 1, 2, \ldots, n),$$

that is,

$$\sum_{i=1}^{n} \frac{q_{ij}}{d_j} A_i = T_j \qquad (j = 1, 2, \ldots, n).$$

We first prove the order of T_j' is d_j. If $d_j = 1$, then $T_j' = 0$ in $G(A)$ and has order 1. Suppose now that $d_j > 1$. Let k be the order of T_j'. Then $k \mid d_j$, since $d_j T_j' = 0$ in $G(A)$. We also have $k > 1$, for $k = 1$ implies $d_j \mid q_{ij}$ $(j = 1, 2, \ldots, n)$ and then $d_j \mid \det Q$, a contradiction.

Now $\{q_{ij}\}_{i=1}^n$ has greatest common divisor 1, since Q is unimodular. So there are integers a_i such that

$$\sum_{i=1}^{n} a_i q_{ij} = 1.$$

Since k is the order of T_j' in $G(A)$, we have

$$kT_j = k\sum_{i=1}^{n} \frac{q_{ij}}{d_j} A_i = 0 \qquad \text{in } G(A),$$

that is, we must have every $k\ q_{ij}/d_j = r_i$, an integer. Then

$$kq_{ij} = d_j r_i,$$

$$\sum_{i=1}^{n} k a_i q_{ij} = \sum_{i=1}^{n} d_j a_i r_i,$$

$$k = d_j \sum_{i=1}^{n} a_i r_i,$$

and now d_j divides k. So $d_j = k$.

We next show that $\{T_i' | d_i > 1\}$ is an independent set in $G(A)$. Suppose that v is the reduced form of

$$\sum_{j=1}^{n} a_j T_j = Ta,$$

where $a = \text{col}\ (a_1, a_2, \ldots, a_n)$. Since $T = AQS^{-1}$, we have

$$Ta = AQS^{-1}a.$$

Recall that if $v \in G(A)$, then $v = 0$ if and only if $v = Aw$ where w is an integral vector. Thus $v = 0$ if and only if $QS^{-1}a$ is integral. Since Q is unimodular, $QS^{-1}a$ is integral if and only if $S^{-1}a = (a_1/d_1, a_2/d_2, \ldots, a_n/d_n)$ is integral. Thus, for integers a_j,

$$\sum_{j=1}^{n} a_j T_j' = 0 \qquad \text{in } G(A)$$

if and only if $d_j | a_j$, for $j = 1, 2, \ldots, n$. Suppose that r is the least integer such that $d_r > 1$. Then $d_1 = \cdots = d_{r-1} = 1$ and $d_i > 1$ for $i \geqslant r$, and we have [in $G(A)$]

$$\sum_{j=1}^{n} a_j T_j' = \sum_{j=r}^{n} a_j T_j'$$

and $\{T_i'\}_{i=r}^n$ is an independent set, as required.

We next show $\{T_i'\}_{i=r}^n$ is a generating set for $G(A)$ (actually, we work with the set $\{T_i'\}_{i=1}^n$).

Suppose $v \in G(A)$, so that v is an integral vector and

$$v = \sum_{i=1}^{n} \frac{a_i}{b_i} A_i = A \operatorname{col}\left(\frac{a_1}{b_1}, \ldots, \frac{a_n}{b_n}\right).$$

Since Q is unimodular, there is a rational vector $r = \operatorname{col}(r_1/s_1, \ldots, r_n/s_n)$ such that

$$AQr = v.$$

But $AQ = TS$, so

$$v = T \operatorname{col}\left(\frac{d_1 r_1}{s_1}, \ldots, \frac{d_n r_n}{s_n}\right).$$

Now v is integral and T is unimodular, so we must have $d_i r_i / s_i = k_i$ for some integers k_i, $i = 1, 2, \ldots, n$. But then

$$v = \sum_{i=1}^{n} k_i T_i' = \sum_{i=r}^{n} k_i T_i' \qquad \text{in } G(A),$$

as required, and $\{T_i'\}_{i=r}^n$ is a generating set for $G(A)$.

(b): Since $\{T_i'\}_{i=r}^n$ is an independent generating set for $G(A)$, and the order of T_i' is d_i, then by definition

$$G(A) \cong \mathbf{Z}_{d_r} \oplus \mathbf{Z}_{d_{r+1}} \oplus \cdots \oplus \mathbf{Z}_{d_n}.$$

We may add on the trivial groups $\mathbf{Z}_{d_1}, \mathbf{Z}_{d_2}, \ldots, \mathbf{Z}_{d_{r-1}}$ to get (b).

(c): The order of $G(A)$ is the product $d_r d_{r+1} \cdots d_n = d_1 d_2 \cdots d_n = D$. ∎

4. THE NUMBER OF INTEGRAL POINTS IN $P(A)$

We use the notation of the preceding sections. Let L be the set of integral points in $P(A)$, and $L_0 = G(A)$.

Let N_k denote the number of elements v of L_0, $v = Ax$, such that x has exactly k zero coordinates.

We first express the cardinality of L in terms of the numbers N_k, and then give a recursion for $\{N_k\}$, which expresses N_k in terms of greatest common divisors of subdeterminants of A. In Sec. 5 we give some examples, one of which shows that $|L|$ is not a similarity invariant.

THEOREM 4.1. *The cardinality of L is given by*

$$|L| = D + \sum_{k=1}^{n} (2^k - 1)N_k.$$

Proof. The points of $L - L_0$ arise in a simple way from the points of L_0, for suppose $v \in L_0$, say

$$v = \sum_{i=1}^{n} x_i A_i = Ax \qquad (0 \leqslant x_i < 1).$$

If x has exactly k zero coordinates, then there are precisely $2^k - 1$ points of $L - L_0$ of the form Ay, where y is the result of replacing one or more of the zero coordinates of x by ones (that is, the reduced form of y is x, for each such y). Every point of $L - L_0$ arises in this way from just one point of L_0, and so the number of points in $L - L_0$ is

$$|L - L_0| = \sum_{k=1}^{n} (2^k - 1)N_k.$$

Since $|L_0| = D$ and $L \cap L_0 = \varnothing$, the theorem is proved. ∎

It is obvious that $N_n = 1$, and we find $N_{n-1}, N_{n-2}, \ldots, N_1$ successively.

DEFINITION 4.2. Let $1 \leqslant k < n$. For each k-tuple $(i_1, i_2, \ldots, i_k)$ with

$$1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n,$$

let $c(i_1, i_2, \ldots, i_k)$ denote the greatest common divisor of the $(n-k) \times (n-k)$ minors of the matrix resulting from A by deleting columns $i_1, i_2, \ldots, i_k$. Let $H(i_1, i_2, \ldots, i_k)$ be the subgroup of $L_0 = G(A)$ consisting of all $v = Ax$ such that x has zeros in positions $i_1, i_2, \ldots, i_k$.

THEOREM 4.3. *The cardinality of* $H(i_1,\dots,i_k)$ *is* $c(i_1,\dots,i_k)$.

Proof. Let A' be the matrix resulting from A by deleting columns $i_1, i_2, \dots, i_k$, and let x' be the vector resulting from x by deleting entries $i_1, i_2, \dots, i_k$. Then $v = Ax \in H(i_1,\dots,i_k)$ if and only if $Ax = A'x'$.

We may define the group $G(A')$ in the obvious way, and it is evident that $G(A') \cong H(i_1,\dots,i_k)$.

There are unimodular matrices P and Q so that

$$PA'Q = \begin{bmatrix} B \\ 0 \end{bmatrix},$$

where $B = \text{diag}\,(c_1, c_2, \dots, c_{n-k})$, $c_i \mid c_{i+1}$. As is well known,

$$c_1 c_2 \cdots c_{n-k} = c(i_1, i_2, \dots, i_k),$$

and this is the cardinality of the group $G(A')$, that is, the cardinality of $H(i_1,\dots,i_k)$. ∎

THEOREM 4.4. $N_n = 1$, *and for* $1 \leqslant k < n$,

$$N_k = \sum c(i_1,\dots,i_k) - \sum \binom{j}{k} N_j$$

where the left-hand sum runs over all k*-tuples* $(i_1,\dots,i_k)$ *with* $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$, *and the right, over* j *satisfying* $1 \leqslant k < j \leqslant n$.

Proof. Clearly $N_n = 1$. Suppose that N_j has been determined for all $j > k$, $1 \leqslant j \leqslant n$. Suppose that $v = Ax$ with exactly $k+t$ coordinates of x equal to zero. Then x is counted $\binom{k+t}{k}$ times by the sum

$$S_k = \Sigma c(i_1,\dots,i_k)$$

[which runs over all k-tuples $(i_1,\dots,i_k)$ with $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$], once for each k-subset of the set of zero-coordinates of x. Thus the count S_k includes a total of $\binom{k+t}{k} N_{k+t}$ points with exactly $k+t$ zero-coordinates, and the result follows. ∎

5. EXAMPLES

EXAMPLE A. A simple example shows that the quantity L is not a similarity invariant.
Put

$$A=\begin{bmatrix}2 & 4\\ 6 & 8\end{bmatrix}, \qquad P=\begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}.$$

Then one checks that

$$B=PAP^{-1}=\begin{bmatrix}-6 & 22\\ -4 & 16\end{bmatrix}.$$

but for A, $L=15$, whereas for B, $L=13$.

EXAMPLE B. In this example, we carry out the computations for the matrix

$$A=\begin{bmatrix}4 & 3 & 1\\ 2 & 1 & 5\\ 6 & 2 & 4\end{bmatrix}.$$

Employing elementary row and column reduction, we find unimodular P, Q:

$$P=\begin{bmatrix}0 & 1 & 0\\ 0 & -2 & 1\\ 1 & -5 & 1\end{bmatrix}, \qquad Q=\begin{bmatrix}0 & 1 & -3\\ 1 & -2 & 11\\ 0 & 0 & -1\end{bmatrix},$$

so that

$$PAQ=\begin{bmatrix}1 & 0 & 0\\ 0 & 2 & 0\\ 0 & 0 & 20\end{bmatrix}.$$

Then $AQ_1=\text{col}\ (3,1,2)$, corresponding to $d_1=1$; $AQ_2=\text{col}\ (-2,0,2)$, corresponding to $d_2=2$; and $AQ_3=\text{col}\ (20,0,0)$, corresponding to $d_3=20$. Then $T_1=\text{col}\ (3,1,2)$ is zero in $G(A)$; $T_2=\text{col}\ (-1,0,1)$ gives an element of order 2

in $G(A)$; and $T_3 = \text{col}\,(1,0,0)$ gives an element of order 20 in $G(A)$, e.g.

$$\text{col}\,(1,0,0) = \frac{-3}{20}A_1 + \frac{11}{20}A_2 + \frac{-1}{20}A_3$$

Then

$$v_3 = \tfrac{17}{20}A_1 + \tfrac{11}{20}A_2 + \tfrac{19}{20}A_3$$

is in $G(A)$ and has order 20. From T_2 we get $v_2 = \frac{1}{2}A_1 \in G(A)$.

Next we compute $c(1,2) = \gcd(1,5,4) = 1$, $c(1,3) = \gcd(3,1,2) = 1$, $c(2,3) = \gcd(4,2,6) = 2$, $c(1) = \gcd(14,10,-6) = 2$, $c(2) = \gcd(18,10,22) = 2$ and $c(3) = \gcd(2,10,2) = 2$. Then

$$N_3 = 1,$$

$$N_2 = c(1,2) + c(1,3) + c(2,3) - \binom{3}{2}N_3 = 1,$$

$$N_1 = c(1) + c(2) + c(3) - \binom{3}{1}N_3 - \binom{2}{1}N_2 = 1.$$

Thus we have one point with two zeros in $G(A)$ (an edge point) and one with one zero (a face point). Then

$$|L| = |\det A| + (2^3 - 1)N_3 + (2^2 - 1)N_2 + (2 - 1)N_1$$

$$= 51.$$

The edge point is $A\,\text{col}(\frac{1}{2},0,0) = \text{col}(2,1,3) = v_2$, and the face point is $A\,\text{col}(0,\frac{1}{2},\frac{1}{2}) = \text{col}(2,3,3) = 10v_3 \oplus v_2$.

REFERENCES

1 Morris Newman, *Integral Matrices*, Academic, New York, 1972.
2 Sam Perlis, *Theory of Matrices*, Addison-Wesley, Reading, Mass., 1958.

Received January 1979; revised 9 April 1979